CIS 100 Introduction to Information Technology

Security, Netiquette, Privacy and Ethics

Security

- Types of hackers and security professionals
  - White hat hackers
    - Computer security experts, penetration testers, ethical hackers, computer forensics experts
  - Black hat hackers
    - Hackers, crackers, script kiddies, cyberterrorists, cyberextortionists (corporate espionage), cybercriminals, identity thieves, financial fraudsters, spies, etc.

Security

- Types of hackers and security professionals
  - Other
    - Cyberbully (harassment), disgruntled employees, hactivist (hacks for social, ideological, political, etc. reasons), vandalists

Security

- Risks
  - Data theft
    - Personal information, health care information, corporate trade secrets, government files, etc.
  - Identity and financial theft
    - Soc. Sec. Number, bank information/money, etc.
  - Other privacy risks
    - Harassment, cell phone information/photos, e-mail, home address, online shopping habits, etc.

Security

- Risks
  - File corruption
    - Viruses, files won't open, computer won't boot, etc.
  - Hardware theft
    - PCs, laptops, monitors, PDAs, etc.
  - Copyright infringement
    - Music, movies, web site content, written word

Security

- Threats
  - Malware
    - Short for malicious software; umbrella for all types: viruses, worms, Trojan horses, etc.
  - Statistics
    - Kaspersky Lab reported that in 2010, 82% of all e-mail was spam. The Message Anti-Abuse Working Groups reports the number between 88-92%.
      http://www.kaspersky.com/news?id=207576277
      http://en.wikipedia.org/wiki/E-mail_spam

Security

- Threats
  - Statistics
    - The number of new malicious programs detected during 2010 was approximately 13 million.
    - The total number of online attacks and local infections recorded in 2010 exceeded 1.9 billion incidents.

    http://www.kaspersky.com/reading_room?chapter=207717661

Security

- Threats
  - Statistics, continued
    - Example of online attack from previous slide
      - "Drive-by-download", e.g. a malicious program that is automatically downloaded to your computer without the user's consent or knowledge, such as through an ActiveX component, that automatically runs when you visit a web page or by clicking a deceptive web page link or pop-up window

Security

- Threats
  - Statistics, continued
    - Phishing using social networking to lure victims increased 1,200 % – from a low of 8.3 % of all phishing in January to a high of 84.5 % in December 2010.
    - Phishing that targeted online gaming sites reached a high of 16.7 % of all phishing in June. http://blogs.technet.com/b/mmpc/archive/2011/05/11/announcing-microsoft-security-intelligence-report-volume-10.aspx

Security

- Threats
  - Statistics, continued
    - Security vendor Palo Alto Networks found that companies had to spend more than $6 billion annually in 2009 on firewall, IPS, proxy and URL filtering products to protect themselves. http://www.techworld.com.au/article/299429/botnets_4_reasons_it_getting_harder_find_fight_them/?pp=2

Security

- Threats
  - Statistics, continued
    - The Mydoom worm first appeared in 2004 for spam purposes, but also contained a Trojan horse backdoor remote access payload, a Distributed DoS attack, blocked user access to Microsoft antivirus web site, and social engineering to lure users to open attachment.
    - For a period of a few hours during the middle of the same day that Mydoom was released, the Internet experienced a performance decline of between 10% and 50% with 1 in 10 e-mail messages containing the worm. Within a few days, it is estimated that 1 in 5 e-mails contained the worm.

Security

- Threats
  - Malware
    - Spam
    - Virus
    - Worm
    - Trojan horse
    - Spyware
    - Rootkit
    - Botnet (and zombies)
  - Intrusion
  - Social engineering
  - Phishing
  - Keylogger
  - Backdoors
  - Hoaxes

Security

- Threats
  - Intrusion
    - Unauthorized access (break in) to a computer system
    - Hacker used to refer to a clever programmer; now it refers to those who exploit security vulnerabilities to break into a system
  - Malware
    - Short for malicious software; umbrella for all types: viruses, worms, trojan horse, etc. to be discussed

Security

- Threats
  - Spam
    - Typically refers to unsolicited/unwanted e-mail (mass e-mailings of junk/advertising)
    - Spam can also come in the form of unwanted contact/message in: instant messaging programs, message boards/forums, blogs, wikis, mobile phone messages, fax machine transmissions and search engine results

Security

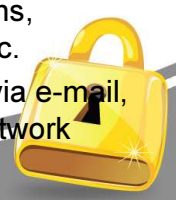
- Threats
  - Spam
    - 80-90% of all e-mail is spam
    - Causes lost productivity, consumes network bandwidth and storage space, and forces companies to spend millions on IT resources to control spam through filters and servers
    - Spam can also contain malware, adware, spyware, botnets, etc.

Security

- Threats
  - Virus
    - A self-replicating program that spreads by inserting copies of itself into other executable code or documents; needs a host file to infect.
    - Transmitted via e-mail, downloaded files, USB thumb drives, files on a network, images, etc.
    - Can damage files, delete files, cause a computer not to boot up, disable certain functionality, etc.
    - Many types: logic bomb, macro virus, file virus, boot virus, resident virus, polymorphic virus, etc.

Security

- Threats
  - Worms
    - Like a virus, a worm is also a self-replicating program
    - A worm differs from a virus in that it propagates through computer networks without user intervention and does not need a host file
    - Unlike a virus, it does not need to attach itself to an existing program; can spread via port scans, backdoors, software/OS vulnerabilities, etc.
    - Like viruses, worms are also transmitted via e-mail, downloaded files, USB drive, files on a network



Security

- Threats
  - Social engineering
    - Act of manipulating someone to do something, such as divulging confidential information, rather than by breaking in or using technical hacking techniques
    - A lie or con
    - Example: impersonating an employee at a company and asking the IT department to divulge or reset your password

Security

- Threats
  - Phishing
    - Phishing is an example of social engineering
    - Mass phishing e-mails are sent pretending to be from your bank, eBay, PayPal, Facebook, or Amazon, for example, informing you that there has been suspicious activity in your account and ask you to log into a web site
    - This web site is a fake one set up to capture your username and password so later left can take place

Security

- Threats
  - Trojan horse
    - A destructive program masquerading as a benign or desirable file/application
    - For example, could be a music media file with a virus inside it
    - Possible Trojan horse payloads:
      - Remote access to your computer
      - Keylogger
      - Modification or deletion of files
      - Watch user's computer screen

Security

- Threats
  - Spyware
    - Type of malware that collects small pieces of information about users without their knowledge
    - Usually do not replicate like worms and viruses
    - May display popup advertisements
    - May cause unwanted increases and usage of CPU, hard drives, RAM, and network
    - May causes computer freezing, inability to use browser/browser hijacking, etc.

Security

- Threats
  - Spyware
    - May cause inability to connect to Internet or inability to run programs to clean the spyware off
    - May get from e-mail spam, downloading a peer-to-peer software such as Kazaa, downloading a program from Internet, or from a web site thorough a web browser exploit/vulnerability

Security

- Threats
  - Rootkit
    - A program that hides in a computer and allows someone continued privileged access to the computer.
    - Rootkits may act as a "keylogger" to steal password or credit card information
    - Rootkits may also act as "backdoor" permitting unauthorized access to computer
    - Example: Sony BMG Music installed hidden software on any computer that played Sony CDs that prevented CDs from being copied.

Security

- Threats
  - Botnet
    - A collection of infected (zombie) computers that have been taken over by hackers and/or malware to perform malicious acts, such as Denial-of-Service (DoS) attacks, generating spam, or installing spyware and adware
    - A botnet's presence on a computer is most often stealth and unknown the user

Security

- Threats
  - Keylogger
    - Software or hardware that tracks and records the user keyboard usage, e.g. typing in your username and password
    - Software-based methods include malware, packet sniffer, or a software available to monitor children's use of computer
    - Hardware-based methods include the 2 GB USB keylogger to the right

Security

- Threats
  - Hoaxes
    - Also known as chain letter or urban legend
    - Typically involves an e-mail sent out with false information intended to make the recipient believe it is true and e-mail it to others
    - May contain images or videos
    - Results in lost employee productivity, consumption of internet bandwidth and storage space, and perpetuation of false information, but could also contain scam/phishing attach

Security

- Threats
  - Hoaxes
    - Examples

Lonelygirl15 (2006)
Series of videos claiming to be by young woman, but were scripted by actress hired by Internet company

Bill Gates Wants to Give You Money (1997)
Chain letter: forward the e-mail you get to others and Gates Foundation will send you money for testing their e-mail tracking program

Hercules the Dog (2007)
"World's Largest Dog"

Security

- Detection
  - Symptoms of viruses
    - File/documents damaged and will not open
    - Files/documents deleted and missing files
    - Computer will not boot up, compute freezes, sluggish or unexpectedly restarts/reboots
    - Certain functionality of the operating system disabled, e.g. firewall, add/remove programs, Internet, etc.
    - Certain applications will not open
    - Excessive hard drive activity
    - Anti-virus program will not run and new one cannot be installed

Security

- Detection
  - Symptoms of spyware
    - Web browser home page is changed
    - You end up at a strange web site every time you perform a web search
    - Loss of Internet connection
    - Your firewall and anti-virus programs are turned off and/or won't run
    - You keep getting pop-ups windows
    - Your computer is running slow
    - New web browser components, such as unknown Toolbars have been installed and cannot be removed

Security

- Prevention
  - Anti-virus software
    - Install and upgrade antivirus software regularly to prevent malware
    - There are also security suites that include: anti-virus, anti-spyware, anti-phishing and firewall capabilities
    - Examples: McAfee AntiVirus, Norton AntiVirus, BitDefender, Microsoft Security Essentials (free)

Security

- Prevention (viruses)
  - Install and update anti-virus software regularly
  - Never open an e-mail unless you are expecting it and it from a trusted source, even if your work has spam filters
  - Scan all downloaded programs and removable media
  - Install a personal firewall software
  - Do not boot from removable media unless you're sure it's uninfected
  - Set applications to warn you before running macros in documents
  - Keep your operating system and web browser up-to-date with the latest patches

Security

- Prevention
  - Spyware removal software
    - If you suspect you have spyware, you should install a spyware removal software (it's a good idea to run periodically anyways)
    - Examples: Lavasoft Ad-Aware, Spybot S&D, Malwarebytes, Spyware Doctor
    - Many of these are free to download and easy to use

Security

- Prevention
  - Phishing toolbar
    - Some web browsers have features that will help detect phishing web sites
    - Microsoft Internet Explorer calls it SmartScreen Filter
    - There are also popup blocker add-ons that can be installed into a web browser to help prevent adware and other potential malware from the web browser

Security

- Prevention
  - E-Mail and Web Browsing Habits
    - Another important method for preventing phishing and other threats (e.g. viruses, spyware, etc.) is education on good, safe web browsing and e-mail habits
    - Do not respond to spam e-mails (you'll get more)
    - Use a disposable e-mail address to sign up for random web registrations in case you get spam
    - Avoid using peer-to-peer file sharing programs such as bittorrent (and inappropriate web sites) as they are a major source of malware

Security

- Prevention
  - E-Mail and Web Browsing Habits, continued
    - Never open attachments from someone you do not know
    - Be cautious about attachments from people you know as Internet worms often blast out e-mails with the worm in it to every e-mail address in a compromised e-mail account holder's address book. The message in the message will even sometimes ask you to help them in some way to get you to download a file or click a link.

Security

- Prevention
  - E-Mail and Web Browsing Habits, continued
    - Never click on links in an e-mail. Instead, copy and paste the URL into your web browser to ensure the link is not redirecting you to a phishing web site
      - Phishing e-mails will often tell you there has been suspicious activity in your PayPal, Amazon, eBay, bank, or similar account and suggest you click on the link to login and check to see if everything is ok. Do not do so. Instead, type the URL into your account manually in the browser.

Security

- Prevention
  - E-Mail and Web Browsing Habits, continued
    - Do not click on pop-ups windows, advertisements, or an sudden web pages/browser tabs that tell you that your computer is inflected with a virus and you need to buy/download their antivirus software
    - Verify your web browser security settings are to medium or high to prevent malware in the form of active content, such as ActiveX, third-party cookies, etc.

Security

- Prevention
  - E-Mail and Web Browsing Habits, continued
    - Do not pass along chain letters and e-mail hoaxes; “if it sounds to good to be true, it probably is”
    - Never enter your social security number, credit card number or other personal information into a web browser unless the URL begins with https:// and the green lock symbol (green for go, red for don’t go).

Security

- Prevention
  - Passwords
    - Choosing a good (“strong”) password for your logins is essential
    - Never give your password to anyone else
    - Do not use information that can be easily guessed, e.g. your child's birthday or a word in the dictionary
    - Used both characters (A-Z) and numbers (0-9)
    - Use mixed case (a-z and A-Z)

Security

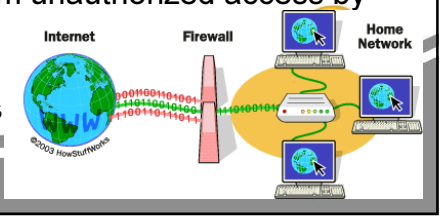
- Prevention
  - Passwords, continued
    - Use special characters such as # @ ! $ -
    - Password length should be at least 8-15 characters, but more is better
    - Use pass-phrases, for example: PapwasaRollingStone
    - In general, character-for-character, password length is more important for security than complexity

Security

- Prevention
  - Passwords, continued
    - Other strategies:
      - You can misspell words. Example: braeKfast2*
      - Consider using a password phrase with mixed case and special character and numeric. Example:
        - » Phrase: You Can Lead a Horse to Water
        - » Password: yclaHtw!1
      - For critical systems, such as a bank account, consider changing your password more often

Security

- Prevention
  - Firewall
    - Install a firewall which, in general terms, is a piece of hardware or software that filters information coming through an Internet connection into a private network or computer system
    - For security, a firewall is used to protect a computer or network from unauthorized access by blocking or filtering unwanted or suspicious transmissions or attacks



Security

- Prevention
  - Firewall, continued
    - Without a firewall in place, your home computer with a direct cable or DSL connection is directly accessible to anyone on the Internet
    - Firewalls can help protect your computer from worms, spyware, keystroke loggers, etc., but should be used in conjunction with anti-virus software, strong passwords, etc.
    - This is called “Defense in Depth”

Security

- Prevention
  - Firewall, continued
    - Your home wireless routers also have firewall capabilities
    - Can also be used to filter access to inappropriate content
    - Firewalls cannot protect your from social engineering, phishing, user initiated downloads that contain malware (trojan horses), e-mail viruses or viruses from USB drives, spam, etc.

Security

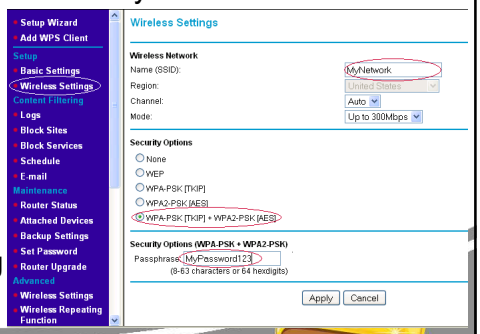
- Prevention
  - Firewall
    - Well-known manufacturers of hardware routers/firewalls
      - Cisco, NetGear, Linksys
    - Well-known software firewalls, also known as Personal Firewalls
      - Zone Alarm, Norton, Kaspersky, McAfee, Trend Micro, Comodo Firewall

Security

- Prevention
  - Encryption
    - Encryption is the process of converting plain-text information into an unreadable format except by those with a special code called a key
    - Used to transmit/communicate secret information
    - Used in web sites, e-mail, operating systems, etc.
    - Make sure whenever you are sending credit card information over the web, the web address (URL) begins with https:// or you run the risk your information can be read while in transmission

Security

- Prevention
  - Encryption, continued
    - Encryption is also used to secure your wireless router
    - Be sure to use to use WPA2 encryption
    - Also, choose a strong password (this one is weak)
    - There is also encryption for operating system files, e-mail, online shopping, etc.



Security

- Prevention
  - Wireless security
    - When setting up a wireless router, be sure to configure the following:
      - Change default Administrator password
      - Change default SSID
      - Enable MAC filtering
      - Choose WPA2 for encryption method
      - Set very strong password
      - Turn off SSID broadcasting

Security

- Prevention
  - Keep software on your computer up-to-date (very important)
    - This includes your: Operating System (such as Windows 7), productivity software like Microsoft Office, e-mail software such as Outlook, your web browser, such as Firefox or Internet Explorer, etc.
    - This is why software makers, such as Microsoft, regularly release Patches, Hotfixes, Updates, etc.
    - These fix bugs and known security vulnerabilities.

Security

- Prevention
  - Biometric
    - Biometric security is used at some companies and government organizations
    - It includes: fingerprint scan, face recognition, palm recognition, iris (eye) scan, voice recognition.
    - Some have concerns: false positives, false negatives, privacy, passwords can be reset – fingerprints cannot, physical assaults to obtain biometric information.

Security

- Prevention
  - Physical security of computer hardware
    - Theft is a major problem at companies, schools, hospitals, government organizations, etc.
    - Desktop, laptops, monitors, LCD projectors, etc.
    - Most schools install computer locks to lock down computer, monitor, projectors, etc.
    - You can also buy a computer lock, setup start-up BIOS password on your computer, never let laptop leave your sight, etc.

Security

- Prevention
  - Backup
    - Always keep up-to-date backups of your data and original CD/DVDs of your software and operating system so you can restore your system in the event of data loss from viruses, malware, hardware failure, hacking, theft, etc.
    - Many methods: external hard drive (good choice), DVD, CD, USB drive (never use as only method), online backup.
    - Update an Off-Site Backup at least once a year.

Security

- Summary of Prevention Measures
  - Use strong passwords
  - Install anti-virus, anti-spyware, and anti-phishing software
  - Install firewall (hardware router and/or personal firewall software)
  - Keep all software and operating system up-to-date with latest updates and patches
  - Follow good/safe web browsing and e-mail habits
  - Use encryption when appropriate
  - Configure your wireless router with secure settings
  - Ensure the physical security of your hardware
  - Use biometric security methods when appropriate
  - Keep up-to-date data and software backups

Netiquette

- Netiquette
  - "Network (or Internet) Etiquette"
    - Guidelines, or set of rules, for good/acceptable online behavior
    - Do's and don't of online communication
  - No shouting, i.e. using all capital letters in e-mails, chat rooms, etc. Is also more difficult to read.
  - No flaming, i.e. posting insulting remarks on forums, discussion boards, chat rooms, etc.
    - Be forgiving other people's mistakes

Netiquette

- Netiquette
  - Do not send Spam
    - Many types: don't forward e-mail hoaxes or chain letters, do not spam message boards, instant messaging (spim), social networking spam, etc.
  - Be careful with the use of Reply All
    - Typically, do not use if original e-mail sent to an e-mail group of hundreds at a company.
    - This clogs up the e-mail systems and wastes everyone's time to read messages.

Netiquette

- Netiquette
  - Be careful on the size of attachment you send
  - Use descriptive Subject lines in e-mails
  - Choose a good/professional e-mail address and write professional e-mails
    - Greeting such as Dear… Sign off Regards, Your Name (i.e. salutation/valediction), use Spell-Check
  - Check to be sure question not already asked if posting a question to a message board/forum

Netiquette

- Netiquette
  - Respect the privacy of others
    - If sending an e-mail to many people who do not know each other, use BCC so you do not reveal all their e-mail address to each other.
    - Do not forward an e-mail unless you have the permission of the original sender; And be careful you are not forwarding dozens of other e-mail addresses if its been a chain e-mail.
    - Do not post others photos online without permission (they're permanent once online).

Privacy

- Many have concerns over privacy with the Internet connecting everyone; It may also help prevent identity and financial theft and stalking
- Privacy guidelines
  - Do not post personal/sensitive information only, e.g. birth date, home address, last name, etc.
  - Be careful what photos you post online – the majority of companies Google potential hires and numerous graduate and medical schools have for applicants
  - Information you post online can be permanent.

Privacy

- Privacy guidelines and tips, continued
  - Use a disposable e-mail address with no personal information in it for web sites that require you to register.
  - Set your web browser to not allow Third-Party Cookies which can track the web sites you visit.
  - Web browsers such as Firefox, have a “Private browsing” feature you can use to not record web pages you visit (History list), etc.
  - Be aware that your web browsing and e-mail at work is not private since you are using company resources and time.

Ethics

- Respect the copyright of online material and content; Give credit to sources when you use them.
- Respect the copyright of computer software, music, and movies, i.e. peer-to-peer programs like Limewire, bittorrent, etc.
- Many netiquette guidelines are also ethical guidelines, e.g. do not flame, do not spam, respect others privacy online, etc.
- Do not access someone else’s e-mail, computer, web sites, USB drive, etc. without permission.